ABSTRACT

A confidential datum, such as a private key used in public key signature systems, is secured in a digital wallet using a "generation camouflaging" technique. With this technique, the private key is not necessarily stored in the digital wallet, not even in an encrypted form. Instead, the wallet contains a private key generation function that reproduces the correct private key when the user inputs his or her pre-selected PIN. If the user inputs an incorrect PIN, an incorrect private key is outputted. Such private key can be configured so that it cannot be readily distinguished from the correct private key through the use of private key formatting, and/or the use of pseudo-public keys corresponding to the private key. The techniques described herein are also applicable to other forms of regeneratable confidential data besides private keys.